Title	The 12-th roots of the discriminant of an elliptic curve and the torsion points; a survey (Algebraic Number Theory and Related Topics 2013)
Author(s)	Yoshikawa, Sho
Citation	数理解析研究所講究録別冊 = RIMS Kokyuroku Bessatsu (2015), B53: 243-248
Issue Date	2015-09
URL	http://hdl.handle.net/2433/241287
Right	© 2015 by the Research Institute for Mathematical Sciences, Kyoto University. All rights reserved.
Type	Departmental Bulletin Paper
Textversion	publisher

RIMS Kôkyûroku Bessatsu
B53 (2015), 243–248

The 12-th roots of the discriminant of an elliptic curve and the torsion points; a survey

By

Sho YOSHIKAWA*

Abstract

This article is a survey of [2], which is a joint work with K. Fukuda. Given an elliptic curve over a scheme with 6 invertible, its discriminant defines a canonical μ_{12}-torsor over the base scheme. In this article, we give an explicit description of this μ_{12}-torsor in terms of the 3-torsion points and of the 4-torsion points of the given elliptic curve. We refer our paper [2] for the detail.

§ 1. Introduction

Throughout this paper, n only takes the value 3 or 4. Let E be an elliptic curve over a scheme S on which n is invertible. We define an étale μ_n-torsor $T_n(\Delta_{E/S})$ associated to the discriminant of E as follows: If E is given by a Weierstrass equation over S, then we can consider the discriminant $\Delta_{E/S}$ of E as an element of $\mathcal{O}(S)^\times/(\mathcal{O}(S)^\times)^n \hookrightarrow \mathrm{H}^1(S, \mu_n)$, and in this case $T_n(\Delta_{E/S})$ is defined to be the étale μ_n-torsor associated to this element. Note that, when S is a spectrum of a field, $T_n(\Delta_{E/S})$ coincides with the μ_n-torsor consisting of n-th roots of the discriminant Δ_E of E. We also remark that, since the discriminant is determined up to an element of $(\mathcal{O}(S)^\times)^{12}$, the above construction makes sense only in the case $n = d$ with d a divisor of 12, and that we have only to consider the cases for $n = 3, 4$ separately. In the general case, Zariski-locally on S, E is given by a Weierstrass equation, and so we can locally define the étale μ_n-torsors attached to E as above. Then, glue them together to define $T_n(\Delta_E/S)$.

Received March 31, 2014. Revised February 23, 2015.
2010 Mathematics Subject Classification(s): 11G02.
Key Words: *elliptic curve, discriminant, combinatorics.*
Supported by the Program for Leading Graduate Schools, MEXT, Japan
*Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1 Komaba Meguro-ku Tokyo 153-8914, Japan.
e-mail: yoshi@ms.u-tokyo.ac.jp

The aim of this article is to construct explicitly another étale μ_n-torsor $T_n(E[n])$ over S from the locally constant étale sheaf $E[n]$ on S, and to construct an isomorphism $w_n : T_n(E[n]) \xrightarrow{\simeq} T_n(\Delta_E)$ of étale μ_n-torsors over S. The construction of this isomorphism is based on the results of Serre [5, 5.5] and Lang-Trotter [4, §11]. Furthermore, we see that, if E is a Tate curve E_q over $\mathbb{Q}((q))$, then the isomorphism coincides with a natural one in the sense that we state in Theorem 3.1.

§ 2. Constructions

Let the notation be as in the introduction. In this section, we explain our constructions of the μ_n-torsor $T_n(E[n])$ over S and of an isomorphism $w_n : T_n(E[n]) \xrightarrow{\simeq} T_n(\Delta_E)$ of étale sheaves on S. For simplicity, we assume that E is given by a Weierstrass equation and that $E[n]$ is constant over S. The general case is easily reduced to this case by étale descent.

For any set I we identify I with the constant étale sheaf of sets on S associated to I. In particular, we will deal with $E[n]$ as if it were an abstract free $\mathbb{Z}/(n)$-module of rank 2.

§ 2.1. Constructions for $n = 3$

Let us denote the projective space associated with $E[3]$ by $\mathbb{P}(E[3]) := (E[3] \setminus \{0\})/\{\pm 1\}$. We define a set $T_3(E[3])$ by

$$T_3(E[3]) = \{\{X, Y\} |\ X \sqcup Y = \mathbb{P}(E[3]), \#X = \#Y = 2\}.$$

Next we define a map w_n. Assume that E is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

Let $b = b_4 = a_3^2 + 4a_6$ be the constant defined in [6, III, §1]. For $\{X, Y\} \in T_3(E[3])$, denote the x-coordinates of the elements in X by x_1 and x_2, and the x-coordinates of the elements in Y by x_3 and x_4. Then, it can be shown that the value

$$w_3(\{X, Y\}) := b_4 - 3(x_1x_2 + x_3x_4) \tag{2.2}$$

is a cubic root of the discriminant of (2.1).

Proposition 2.1. *Let the notation be as above. Then,* (2.2) *induces an isomorphism* $w_3 : T_3(E[3]) \to T_3(\Delta_E)$ *of constant sheaves over* S. *Moreover,* w_3 *is independent of the choice of a Weierstrass equation for* E.

§ 2.2. Constructions for $n = 4$

Let $S_4(E[4])$ denote a set defined by

$$\big\{(P, Q, R) \in E[4] \times E[4] \times E[4] \,|\, \{2P, 2Q, 2R\} = E[2] \setminus 0\big\}.$$

For each $\sigma \in \mathfrak{S}_3$, define an involution $[\sigma]$ of $S_4(E[4])$ by $[\sigma](P_1, P_2, P_3) := (P'_1, P'_2, P'_3)$ with

$$P'_{\sigma(1)} = P_{\sigma(1)}, P'_{\sigma(2)} = P_{\sigma(2)} + 2P_{\sigma(1)}, \text{ and } P'_{\sigma(3)} = P_{\sigma(3)}.$$

Since $[\sigma]$'s commute with each other, we obtain an action of $\mathbb{F}_2^{\mathfrak{S}_3}$ on $S_4(E[4])$. Combining this action with a canonical action of $\mathfrak{S}_3$ on $S_4(E[4])$ by the permutations, we obtain an action of $G := \mathfrak{S}_3 \ltimes \mathbb{F}_2^{\mathfrak{S}_3}$ on $S_4(E[4])$. Here, the left action of $\mathfrak{S}_3$ on $\mathbb{F}_2^{\mathfrak{S}_3}$ defining the semi direct product is given by $\tau \cdot [\sigma] = [\tau\sigma]$ for $\sigma, \tau \in \mathfrak{S}_3$. Let N be the kernel of the composite

$$p : \mathbb{F}_2^{\mathfrak{S}_3} \to \mathbb{F}_2^{\mathfrak{A}_3} \to \{\pm 1\},$$

where the first map is the restriction to $\mathfrak{A}_3$ and the second map is the one sending $\sum a_\sigma[\sigma]$ to $(-1)^{\sum a_\sigma}$. Since the action of $\mathfrak{S}_3$ on $\mathbb{F}_2^{\mathfrak{S}_3}$ defining the semi direct product induces an action of $\mathfrak{A}_3$ on N, we obtain $H := \mathfrak{A}_3 \ltimes N \lhd G$.

Definition 2.2. Under the above setting, define the set $T_4(E[4])$ by the quotient

$$T_4(E[4]) := H \setminus S_4(E[4]).$$

The equivalence class of $(P, Q, R) \in S_4(E[4])$ is denoted by $[P, Q, R] \in T_4(E[4])$.

To define a morphism w_4, since we assume here that 4 is invertible on S, we can take a Weierstrass equation for E of the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

For $(P, Q, R) \in S_4(E[4])$, set

$$P' = P + 2Q, Q' = Q + 2R, R' = R + 2P.$$

It turns out that the value

$$\tilde{w}_4(P, Q, R) := 2\frac{y_P - y_{P'}}{x_P - x_{P'}} \cdot \frac{y_Q - y_{Q'}}{x_Q - x_{Q'}} \cdot \frac{y_R - y_{R'}}{x_R - x_{R'}}$$

makes sense on S, and we obtain the following result similar to Proposition 2.1:

Proposition 2.3. *In the above setting, the map $(P, Q, R) \mapsto \tilde{w}_4(P, Q, R)$ induces an isomorphism $w_4 : T_4(E[4]) \xrightarrow{\simeq} T_4(\Delta_E)$ of constant sheaves on S.*

§ 2.3. A μ_n-action on $T_n(E[n])$

To define a μ_n-action, we need the following two lemmas:

Lemma 2.4. *There exists a unique isomorphism $\varphi_n : \bigwedge^2 E[n] \xrightarrow{\simeq} SL(E[n])^{\mathrm{ab}}$ of groups sending $P \wedge Q$ to $\varphi_{P,Q}$ for any basis (P, Q) of $E[n]$.*

In the following lemma, $\mathfrak{A}(\mathrm{Aut}(T_3(E[3])))$ denotes the alternating subgroup of $\mathrm{Aut}(T_3(E[3]))$, and $C(-1)$ the unique cyclic subgroup of $\mathrm{Aut}(T_4(E[4]))$ characterized by the conditions:
(1) $C(-1)$ is contained in the centralizer of $-1 : E[4] \to E[4]$, and
(2) $-1 \in C(-1)$.

Lemma 2.5. *The canonical action of $GL(E[n])$ on $T_n(E[n])$ induces isomorphisms $SL(E[3])^{\mathrm{ab}} \xrightarrow{\simeq} \mathfrak{A}(\mathrm{Aut}(T_3(E[3])))$ and $SL(E[4])^{\mathrm{ab}} \xrightarrow{\simeq} C(-1)$.*

We define a μ_n-action on $T_n(E[n])$ as the compositions:

$$\mu_n \xrightarrow[e_n^{-1}]{\simeq} \bigwedge^2 E[n] \xrightarrow[\text{Lemma 2.4}]{\simeq} SL(E[n])^{\mathrm{ab}} \xrightarrow[\text{Lemma 2.5}]{} \mathrm{Aut}(T_n(E[n])),$$

where e_n is the normalized Weil pairing in the sense of [1, VII, 1, 16] and [2].

§ 3. The Tate curve case

Let K be the complete discrete valued field $\mathbb{Q}((q))$ and $E = E_q$ be the Tate curve associated to the pair (K, q). Then $E(\bar{K})$ is identified with $\bar{K}^\times / q^{\mathbb{Z}}$. Denote by $T_n(q)$ the μ_n-torsor consisting of n-th roots of q. We define a canonical isomorphism

$$\begin{aligned} D : T_n(q) &\longrightarrow T_n(\Delta_E) \\ z &\longmapsto z \prod_{m \geq 1} (1 - q^m)^{\frac{24}{n}} \end{aligned}$$

of μ_n-torsors over K. We also define a map

$$T : T_n(q) \longrightarrow T_n(E[n])$$

by $T(z) = \{\{\omega, z\}, \mathbb{P}(E[3]) \setminus \{\omega, z\}\}$ (resp. $[z, i, (iz)^{-1}]$) for $n = 3$ (resp. 4), where ω (resp. i) is a primitive cubic (resp. 4th) root of unity in $\bar{K}$. It is directly checked from the definition of $T_n(E[n])$ that the map T is independent of the choice of ω and i. In [2], we see that the map T is an isomorphism of μ_n-torsors over K. The following theorem will be crucial to our proof of the main theorem (Theorem 4.1).

Theorem 3.1. *The equality $w_n = D \circ T^{-1} : T_n(E[n]) \to T_n(\Delta_E)$ holds. In particular, w_n is an isomorphism of μ_n-torsors.*

Actually, this theorem is trivial for $n = 3$ since $\mu_3(K) = \{1\}$ implies that a map $T_3(E[3]) \to T_3(\Delta_E)$ of μ_3-torsors is uniquely determined. However, if $n = 4$, we can say that a map $T_4(E[4]) \to T_4(q)$ of μ_4-torsors is determined up to ± 1 since $\mu_4(K) = \{\pm 1\}$. Thus, to prove that w_n coincides with $D \circ T^{-1}$, we have to investigate them more carefully. To do this, it is important to choose a Laurent series field as the base field; in [2], we compute the Laurent series expansion of $w_4([z, i, (iz)^{-1}])$ with $z^n = q$.

§ 4. Main results

We now state our main theorem:

Theorem 4.1. *Let $n = 3$ or 4. There exists a unique way to attach to every elliptic curve E/S with n invertible on S an isomorphism*

$$W_n : T_n(E[n]) \longrightarrow T_n(\Delta_E)$$

of μ_n-torsors over S in the way that W_n satisfies the following two conditions:
(1) Attaching W_n to E/S is compatible with any base change.
(2) If $E = E_q$ is a Tate curve over $\mathbb{Q}((q))$, then W_n coincides with $D \circ T^{-1}$ as in Theorem 3.1.

We want to take w_n defined in Section 2 as W_n. We only give a comment on how to prove that w_n is μ_n-equivariant and that it is uniquely characterized by the conditions (1) and (2). Suppose we have an elliptic curve E/S. Considering étale locally on S, we may assume that E is given by a Weierstrass equation and the étale sheaf $E[n]$ on S is constant. Since our w_n obviously satisfies (1), we may furthermore assume that E is the universal elliptic curve over the modular curve $Y(n)/\mathbb{Z}[1/n]$ of level n. By the connectedness of $Y(n)$, we see that the single point on $Y(n)$ corresponding to a pair $(E_q, (\zeta_n, q^{1/n}))$ and the condition (2) determine w_n for E/S uniquely, and that the μ_n-equivariance of w_n for E/S is deduced from that of Tate curve case (Theorem 3.1). For the detail, see [2].

As an immediate application of Theorem 4.1, we can prove an analogy of Coates' result [3, appendix] to general characteristic cases:

Corollary 4.2. *Let E and E' be elliptic curves over a field K of characteristic* $\mathrm{char}(K) \neq 2, 3$, *and $\varphi : E \to E'$ be an isogeny over K. If $d = \deg\varphi$ is prime to* 12, *then we have $\Delta_E = (\Delta_{E'})^d$ in $K^\times/(K^\times)^{12}$.*

References

[1] P. Deligne, M. Rapoport, *Les schemas de modules de courbes elliptiques*, Modular functions of one variables, II (Proc Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 143-316. Lecture Notes in Math., Vol.349, Springer, Berlin, 1973.

[2] K. Fukuda, S. Yoshikawa, The 12-th roots of the discriminant of an elliptic curve and the torsion points, submitted.

[3] J. Coates, Elliptic curves with complex multiplication and Iwasawa theory, Bulletin of the LMS 23, 321-350, 1991.

[4] S. Lang, H. Trotter, Frobenius Distributions in GL_2-Extensions, Lecture Notes in Math. 504, Springer-Verlag, 1976.

[5] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math., 15: 259-331, 1972.

[6] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math., Springer, 106, 1986.